AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A cooperative spam processing system comprising:

a plurality of e-mail clients communicatively linked to one another;

a plurality of cooperative spam control processors, each of said plurality of cooperative spam control processors coupled to a corresponding one of said e-mail clients, wherein said plurality of cooperative spam control processors are configured to detect spam and to notify others of said plurality of cooperative spam control processors of said spam; and,

a first group administrator for a common group of e-mail clients, said first group administrator establishes an agreement with a second group administrator for a different group of e-mail clients for the exchange of spam notifications between members of said common group and members of said different group, said members of said different group having respective cooperative spam control processors; and,

at least one member of said common group exchanges said spam notifications with at least one member of said different group based on said agreement, wherein,

said agreement establishes a policy that determines which level of trust to apply to spam notifications emanating from other ones of the computing groups.

Claims 2.-4 (Cancelled).

5. (Currently Amended) A cooperative spam control method comprising the steps of:

accepting an electronic spam notification received from a peer e-mail recipient in a common computing group having a first group administrator, said spam notification identifying a spam message received by said peer e-mail recipient;

storing, in a memory device, said spam notification;

if an e-mail is subsequently received which corresponds to said identified spam message, processing, within a cooperative spam control processor of a computer, said received e-mail as spam; and,

consulting a peer policy, stored in said memory device, for said peer e-mail recipient comprising rules for handling e-mail identified as spam by said peer e-mail recipient;

obeying said spam notification if said rules indicate that spam notifications from said peer e-mail recipient are to be obeyed;

ignoring said spam notification if said rules indicate that spam notifications from said peer e-mail recipient are to be ignored;

overriding said spam notification where said e-mail message meets criteria established in said policy for overriding a spam notification;

establishing an agreement between said first group administrator and a second group administrator for a different group of e-mail clients for the exchange of spam notifications between members of said common group and members of said different group, said members of said different group having respective cooperative spam control processors;

forwarding spam notifications from individual peer e-mail recipients in said common computing group to said members of said different computing group based on a level of trust provided for in said agreement;

receiving spam notifications from members of said different computing group based on said agreement; and,

storing said received spam notifications in memory devices of individual peer e-mail recipients of said common computing group.

Claims 6-8 (Cancelled).

9. (Previously Presented) The method of claim 5, wherein said consulting step comprises the step of consulting an internally managed local peer policy.

10. (Previously Presented) The method of claim 5, wherein said consulting step comprises the step of consulting a centrally managed remote peer policy.

Claim 11 (Cancelled)

12. (Currently Amended) A machine readable storage having stored thereon a computer program for cooperative spam control, the computer program comprising a routine set of instructions which when executed by a machine cause the machine to perform the steps of:

accepting an electronic spam notification received from a peer e-mail recipient in a common computing group having a first group administrator, said spam notification identifying a spam message received by said peer e-mail recipient;

storing, in a memory device, said spam notification;

if an e-mail is subsequently received which corresponds to said identified spam message, processing, within a cooperative spam control processor of a computer, said received e-mail as spam; and,

consulting a peer policy, stored in said memory device, for said peer e-mail recipient comprising rules for handling e-mail identified as spam by said peer e-mail recipient;

obeying said spam notification if said rules indicate that spam notifications from said peer e-mail recipient are to be obeyed;

ignoring said spam notification if said rules indicate that spam notifications from said peer e-mail recipient are to be ignored;

overriding said spam notification where said e-mail message meets criteria established in said policy for overriding a spam notification;

establishing an agreement between said first group administrator and a second group administrator for a different group of e-mail clients for the exchange of spam notifications between members of said common group and members of said different group, said members of said different group having respective cooperative spam control processors;

forwarding spam notifications from individual peer e-mail recipients in said common computing group to said members of said different computing group based on a level of trust provided for in said agreement;

receiving spam notifications from members of said different computing group based on said agreement; and,

storing said received spam notifications in memory devices of individual peer e-mail recipients of said common computing group.

Claims 13-15 (Cancelled).

16. (Previously Presented) The machine readable storage of claim 12, wherein said consulting step comprises the step of consulting an internally managed local peer policy.

17. (Previously Presented) The machine readable storage of claim 12, wherein said consulting step comprises the step of consulting a centrally managed remote peer policy.

Claim 18 (Cancelled)

Claim 19 (Cancelled)

20. (Previously Presented) The system of claim 19, wherein said level of trust is at the same level as those notifications emanating from within a respective computing group.

21. (Previously Presented) The system of claim 19, wherein said level of trust is at a lower level than those spam notifications emanating from within a respective computing group.

22. (Previously Presented) The system of claim 1, wherein said first group administrator authorizes and controls membership in said common group of e-mail clients.

23. (Previously Presented) The method of claim 5, wherein said agreement establishes a policy that determines which level of trust to apply to spam notifications emanating from other ones of the computing groups.

24. (Previously Presented) The method of claim 23, wherein said level of trust is at the same level as those notifications emanating from within a respective computing group.

25. (Previously Presented) The method of claim 23, wherein said level of trust is at a lower level than those spam notifications emanating from within a respective computing group.

26. (Previously Presented) The method of claim 5, wherein said first group administrator authorizes and controls membership in said common group of e-mail clients.

27. (Previously Presented) The machine readable storage of claim 12, wherein said agreement establishes a policy that determines which level of trust to apply to spam notifications emanating from other ones of the computing groups.

28. (Previously Presented) The machine readable storage of claim 27, wherein said level of trust is at the same level as those notifications emanating from within a respective computing group.

29. (Previously Presented) The machine readable storage of claim 27, wherein said level of trust is at a lower level than those spam notifications emanating from within a respective computing group.

30. (Previously Presented) The machine readable storage of claim 12, wherein said first group administrator authorizes and controls membership in said common group of e-mail clients.